

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideyuki SUZUKI

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: WIRELESS ADHOC COMMUNICATION SYSTEM, TERMINAL, AUTHENTICATION METHOD FOR USE IN TERMINAL, ENCRYPTION METHOD, TERMINAL MANAGEMENT METHOD, AND PROGRAM FOR ENABLING TERMINAL TO PERFORM THOSE METHODS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

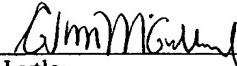
COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-026545	February 3, 2003

Certified copies of the corresponding Convention Application(s)

- are submitted herewith
- will be submitted prior to payment of the Final Fee
- were filed in prior application Serial No. filed
- were submitted to the International Bureau in PCT Application Number Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- (B) Application Serial No.(s)
- are submitted herewith
- will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Registration No. 40,073

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124

804P0181VS00

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日 2003年 2月 3日
Date of Application:

出願番号 特願2003-026545
Application Number:

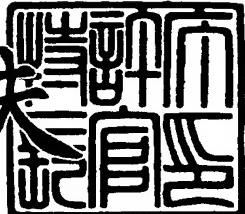
[ST. 10/C] : [JP2003-026545]

出願人 ソニー株式会社
Applicant(s):

2003年12月11日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 0390008020
【提出日】 平成15年 2月 3日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/14
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 鈴木 英之
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代理人】
【識別番号】 100112955
【弁理士】
【氏名又は名称】 丸島 敏一
【手数料の表示】
【予納台帳番号】 172709
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0206900
【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線アドホック通信システム、端末、その端末における認証方法、暗号化方法及び端末管理方法並びにそれらの方法を端末に実行させるためのプログラム

【特許請求の範囲】

【請求項 1】 複数の端末により構成される無線アドホック通信システムであって、

　フレームに認証ヘッダを付して当該フレームを送信する第1の端末と、
　前記フレームを受信して前記認証ヘッダが正当であることを確認する第2の端末とを具備し、

　前記第1の端末は前記第2の端末との間の認証ヘッダ鍵を用いて前記認証ヘッダを生成し、

　前記第2の端末は前記認証ヘッダ鍵を用いて前記認証ヘッダが正当であることを確認する

ことを特徴とする無線アドホック通信システム。

【請求項 2】 複数の端末により構成される無線アドホック通信システムであって、

　第1のフレームのペイロードを暗号化して第1の認証ヘッダを付して当該第1のフレームを送信する第1の端末と、

　前記第1のフレームを受信して前記第1の認証ヘッダが正当であることを確認すると前記暗号化されたペイロードを含む第2のフレームに第2の認証ヘッダを付して当該第2のフレームを送信する第2の端末と、

　前記第2のフレームを受信して前記第2の認証ヘッダが正当であることを確認すると前記暗号化されたペイロードを復号する第3の端末とを具備し、

　前記第1の端末は、前記第3の端末との間の暗号鍵を用いて前記ペイロードを暗号化し、前記第2の端末との間の第1の認証ヘッダ鍵を用いて前記第1の認証ヘッダを生成するものであり、

　前記第2の端末は、前記第1の認証ヘッダ鍵を用いて前記第1の認証ヘッダが正当であることを確認し、前記第3の端末との間の第2の認証ヘッダ鍵を用いて

前記第2の認証ヘッダを生成するものであり、

前記第3の端末は、前記第2の認証ヘッダ鍵を用いて前記第2の認証ヘッダが正当であることを確認し、前記第1の端末との間の前記暗号鍵を用いて前記ペイロードを復号するものである

ことを特徴とする無線アドホック通信システム。

【請求項3】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手段と、

抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか否かを確認する手段と

を具備することを特徴とする端末。

【請求項4】 他の端末の端末識別子に対応して当該他の端末にフレームを到達させるための転送先端末識別子を保持する経路リストを少なくとも一つ有する経路テーブルと、

前記認証ヘッダが正当であり且つ前記フレームの終点端末識別子が当該端末の端末識別子でない場合には前記終点端末識別子を含む前記経路リストを前記経路テーブルから検索して対応する前記転送先端末識別子に対して前記フレームを送信し、前記認証ヘッダが正当でない場合には前記フレームを破棄する手段とをさらに具備することを特徴とする請求項3記載の端末。

【請求項5】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手段と、

抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか否かを確認する手段と、

前記認証ヘッダが正当であり且つ前記フレームの終点端末識別子が当該端末の

端末識別子である場合前記フレームの始点端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵を抽出する手段と、

前記抽出されたユニキャスト暗号鍵により前記フレームのペイロードを復号する手段と

を具備することを特徴とする端末。

【請求項 6】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、

送信しようとするフレームの受信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵により認証ヘッダを生成して前記フレームに付する手段と、

前記フレームを送信する手段と
を具備することを特徴とする端末。

【請求項 7】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、

送信しようとするフレームの受信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵により認証ヘッダを生成して前記フレームに付する手段と、

前記フレームの終点端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵により前記フレームのペイロードを暗号化する手段と、

前記フレームを送信する手段と
を具備することを特徴とする端末。

【請求項 8】 ネットワークを形成する端末のうち直接通信可能な端末の端末識別子を保持する近隣端末リストテーブルと、

前記ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブ

ルと、

前記近隣端末リストテーブルに端末識別子が保持される端末において前記ネットワークからの脱退が発生した場合、その脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから削除する手段とを具備することを特徴とする端末。

【請求項 9】 前記近隣端末リストテーブルに端末識別子が保持される端末において前記ネットワークからの脱退が発生した場合、前記ネットワークを形成する他の端末に対して前記脱退した端末の端末識別子を知らせる端末脱退メッセージを送信する手段

をさらに具備することを特徴とする請求項 8 記載の端末。

【請求項 10】 ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、

前記ネットワークを脱退した端末の端末識別子を知らせる端末脱退メッセージを受信した場合その脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから削除する手段とを具備することを特徴とする端末。

【請求項 11】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、

抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか否かを確認する手順と

を具備することを特徴とする認証方法。

【請求項 12】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リス

トテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、
抽出された前記認証ヘッダ鍵を前記フレームの所定領域と共にハッシュした鍵
付ハッシュ値を生成する手順と、
前記鍵付ハッシュ値と前記フレームの認証ヘッダとを比較することにより前記
認証ヘッダが正当であるか否かを確認する手順と
を具備することを特徴とする認証方法。

【請求項 13】 他の端末の端末識別子に対応して前記他の端末との間の認
証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ
有する鍵管理リストテーブルを備える端末において、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リス
トテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、
抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか
否かを確認する手順と、

前記認証ヘッダが正当であり且つ前記フレームの終点端末識別子が当該端末の
端末識別子である場合前記フレームの始点端末識別子を含む前記鍵管理リストを
前記鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵を抽出
する手順と、

前記抽出されたユニキャスト暗号鍵により前記フレームのペイロードを復号す
る手順と
を具備することを特徴とする暗号化方法。

【請求項 14】 他の端末の端末識別子に対応して前記他の端末との間の認
証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブ
ルを備える端末において、

送信しようとするフレームの受信端末識別子を含む前記鍵管理リストを前記鍵
管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、
抽出された前記認証ヘッダ鍵を前記フレームの所定領域と共にハッシュした鍵
付ハッシュ値を生成して認証ヘッダとして前記フレームに付する手順と、

前記フレームを送信する手順と
を具備することを特徴とする暗号化方法。

【請求項 15】 ネットワークを形成する端末のうち直接通信可能な端末の端末識別子を保持する近隣端末リストテーブルと、前記ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルとを備える端末において、

前記近隣端末リストテーブルに端末識別子が保持される端末における前記ネットワークからの脱退を検出する手順と、

その脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから削除する手順と、

前記ネットワークを形成する他の端末に対して前記脱退した端末の端末識別子を知らせる端末脱退メッセージを送信する手順と
を具備することを特徴とする端末管理方法。

【請求項 16】 ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、

前記ネットワークを脱退した端末の端末識別子を知らせる端末脱退メッセージを受信する手順と、

前記脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから削除する手順と
を具備することを特徴とする端末管理方法。

【請求項 17】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、

抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか否かを確認する手順と
を実行させることを特徴とするプログラム。

【請求項 18】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブ

ルを備える端末に、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、

抽出された前記認証ヘッダ鍵を前記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成する手順と、

前記鍵付ハッシュ値と前記フレームの認証ヘッダとを比較することにより前記認証ヘッダが正当であるか否かを確認する手順と
を実行させることを特徴とするプログラム。

【請求項 19】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、

受信したフレームの送信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、

抽出された前記認証ヘッダ鍵により前記フレームの認証ヘッダが正当であるか否かを確認する手順と、

前記認証ヘッダが正当であり且つ前記フレームの終点端末識別子が当該端末の端末識別子である場合前記フレームの始点端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記ユニキャスト暗号鍵を抽出する手順と、

前記抽出されたユニキャスト暗号鍵により前記フレームのペイロードを復号する手順と

を実行させることを特徴とするプログラム。

【請求項 20】 他の端末の端末識別子に対応して前記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、

送信しようとするフレームの受信端末識別子を含む前記鍵管理リストを前記鍵管理リストテーブルから検索して対応する前記認証ヘッダ鍵を抽出する手順と、

抽出された前記認証ヘッダ鍵を前記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成して認証ヘッダとして前記フレームに付する手順と、

前記フレームを送信する手順と
を実行させることを特徴とするプログラム。

【請求項 2 1】 ネットワークを形成する端末のうち直接通信可能な端末の
端末識別子を保持する近隣端末リストテーブルと、前記ネットワークを形成する
端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リ
ストを少なくとも一つ有する鍵管理リストテーブルとを備える端末に、

前記近隣端末リストテーブルに端末識別子が保持される端末における前記ネッ
トワークからの脱退を検出する手順と、

その脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテ
ーブルから削除する手順と、

前記ネットワークを形成する他の端末に対して前記脱退した端末の端末識別子
を知らせる端末脱退メッセージを送信する手順と
を実行させることを特徴とするプログラム。

【請求項 2 2】 ネットワークを形成する端末の端末識別子に対応して当該
端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管
理リストテーブルを備える端末に、

前記ネットワークを脱退した端末の端末識別子を知らせる端末脱退メッセージ
を受信する手順と、

前記脱退した端末の端末識別子を含む前記鍵管理リストを前記鍵管理リストテ
ーブルから削除する手順と
を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、無線アドホック通信システムに関し、特に認証された端末から送信
されたフレームであることを端末間で確認しながら通信を行う無線アドホック通
信システム、当該システムにおける端末、および、これらにおける認証方法、暗
号化方法及び端末管理方法ならびにそれらの方法をコンピュータ（端末）に実行
させるプログラムに関する。

【0002】

【従来の技術】

電子機器の小型化、高性能化が進み、簡単に持ち運び利用することが可能となつたことから、必要になったその場で端末をネットワークに接続し、通信を可能とする環境が求められている。その一つとして、必要に応じて一時的に構築されるネットワーク、すなわち無線アドホックネットワーク技術の開発が進められている。この無線アドホックネットワークでは、特定のアクセスポイントを設けることなく、各端末（例えば、コンピュータ、携帯情報端末（PDA：Personal Digital Assistance）、携帯電話等）が自律分散して相互に接続される。

【0003】

従来の無線LAN（ローカルエリアネットワーク）環境では、特定のアクセスポイントを設けてそのアクセスポイントと端末との間で無線通信を行っているため、その無線区間においてフレームの暗号化をすれば足りる。例えば、無線LANの暗号化仕様におけるWEP（Wired Equivalent Privacy）では、暗号鍵を用いてフレームを暗号化しておき、アクセスポイントでフレームを復号する際にCRC（Cyclic Redundancy Check）のチェックをすることにより、認証されていない端末からのフレームを破棄するようにしている（例えば、特許文献1参照。）。

【0004】

【特許文献1】

特開2001-111544号公報（図3）

【0005】

【発明が解決しようとする課題】

上述の無線LANでは無線区間がアクセスポイントと端末の間に限られているが、無線アドホック通信システムではネットワークトポロジーが全て無線媒体で形成される。従って、無線アドホック通信システムでは複数の無線リンクをホップさせてフレームを配達する場合が生じるため、無線リンク毎に暗号化処理および復号処理を繰り返すことにより各端末に負荷を与え、計算資源を浪費するおそ

れがある。また、認証されていない端末からのフレームを複数の端末間で配達していくことは本来不要な通信を引き起こすため、無線資源を浪費するおそれがある。

【0006】

そこで、本発明の目的は、無線アドホック通信システムにおいて、配達にかかる端末間でフレーム送信元認証を行うことにある。特に、本発明は、ネットワークを構成する全ての無線端末が管理情報（例えば、ビーコン等）を送信する無線ネットワークにおいて有用である。

【0007】

【課題を解決するための手段】

上記課題を解決するために本発明の請求項1記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、フレームに認証ヘッダを付して当該フレームを送信する第1の端末と、上記フレームを受信して上記認証ヘッダが正当であることを確認する第2の端末とを具備し、上記第1の端末は上記第2の端末との間の認証ヘッダ鍵を用いて上記認証ヘッダを生成し、上記第2の端末は上記認証ヘッダ鍵を用いて上記認証ヘッダが正当であることを確認する。これにより、第1の端末において認証ヘッダ鍵を用いて生成された正当な認証ヘッダが付されたものであることを、第2の端末において確認できるという作用をもたらす。

【0008】

また、本発明の請求項2記載の無線アドホック通信システムは、複数の端末により構成される無線アドホック通信システムであって、第1のフレームのペイロードを暗号化して第1の認証ヘッダを付して当該第1のフレームを送信する第1の端末と、上記第1のフレームを受信して上記第1の認証ヘッダが正当であることを確認すると上記暗号化されたペイロードを含む第2のフレームに第2の認証ヘッダを付して当該第2のフレームを送信する第2の端末と、上記第2のフレームを受信して上記第2の認証ヘッダが正当であることを確認すると上記暗号化されたペイロードを復号する第3の端末とを具備し、上記第1の端末は、上記第3の端末との間の暗号鍵を用いて上記ペイロードを暗号化し、上記第2の端末との

間の第1の認証ヘッダ鍵を用いて上記第1の認証ヘッダを生成するものであり、上記第2の端末は、上記第1の認証ヘッダ鍵を用いて上記第1の認証ヘッダが正当であることを確認し、上記第3の端末との間の第2の認証ヘッダ鍵を用いて上記第2の認証ヘッダを生成するものであり、上記第3の端末は、上記第2の認証ヘッダ鍵を用いて上記第2の認証ヘッダが正当であることを確認し、上記第1の端末との間の上記暗号鍵を用いて上記ペイロードを復号するものである。これにより、第1の端末と第2の端末との間および第2の端末と第3の端末との間では認証ヘッダによるフレーム送信元認証を行う一方で、第1の端末と第3の端末のみが有する暗号鍵でペイロードを暗号化することにより、中間の第2の端末に対してペイロードの秘匿性を担保するという作用をもたらす。

【0009】

また、本発明の請求項3記載の端末は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手段と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手段とを具備する。これにより、受信したフレームに付された認証ヘッダが正当な送信端末により生成されたものであることを受信端末に確認させるという作用をもたらす。

【0010】

また、本発明の請求項4記載の端末は、請求項3記載の端末において、他の端末の端末識別子に対応して当該他の端末にフレームを到達させるための転送先端末識別子を保持する経路リストを少なくとも一つ有する経路テーブルと、上記認証ヘッダが正当であり且つ上記フレームの終点端末識別子が当該端末の端末識別子でない場合には上記終点端末識別子を含む上記経路リストを上記経路テーブルから検索して対応する上記転送先端末識別子に対して上記フレームを送信し、上記認証ヘッダが正当でない場合には上記フレームを破棄する手段とをさらに具備する。これにより、受信したフレームに付された認証ヘッダが正当な送信端末により生成されたものであることが確認された場合には次の転送先端末にフレーム

を転送させ、認証ヘッダが正当でなければそのフレームを破棄させるという作用をもたらす。

【0011】

また、本発明の請求項5記載の端末は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手段と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手段と、上記認証ヘッダが正当であり且つ上記フレームの終点端末識別子が当該端末の端末識別子である場合上記フレームの始点端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を抽出する手段と、上記抽出されたユニキャスト暗号鍵により上記フレームのペイロードを復号する手段とを具備する。これにより、始点端末と終点端末との間で定められたユニキャスト暗号鍵によりペイロードを暗号化して、中間の端末に対してペイロードの秘匿性を担保するという作用をもたらす。

【0012】

また、本発明の請求項6記載の端末は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、送信しようとするフレームの受信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵により認証ヘッダを生成して上記フレームに付する手段と、上記フレームを送信する手段とを具備する。これにより、認証ヘッダ鍵を用いて生成された認証ヘッダが付されていることをフレーム受信端末において確認させるという作用をもたらす。

【0013】

また、本発明の請求項7記載の端末は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、送信しようとするフレーム

の受信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵により認証ヘッダを生成して上記フレームに付する手段と、上記フレームの終点端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵により上記フレームのペイロードを暗号化する手段と、上記フレームを送信する手段とを具備する。これにより、始点端末と終点端末との間で定められたユニキャスト暗号鍵によりペイロードを暗号化して、中間の端末に対してペイロードの秘匿性を担保するという作用をもたらす。

【0014】

また、本発明の請求項8記載の端末は、ネットワークを形成する端末のうち直接通信可能な端末の端末識別子を保持する近隣端末リストテーブルと、上記ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、上記近隣端末リストテーブルに端末識別子が保持される端末において上記ネットワークからの脱退が発生した場合、その脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手段とを具備する。これにより、脱退した近隣端末に関する情報を鍵管理リストテーブルから削除して、未認証状態にするという作用をもたらす。

【0015】

また、本発明の請求項9記載の端末は、請求項8記載の端末において、上記近隣端末リストテーブルに端末識別子が保持される端末において上記ネットワークからの脱退が発生した場合、上記ネットワークを形成する他の端末に対して上記脱退した端末の端末識別子を知らせる端末脱退メッセージを送信する手段をさらに具備する。これにより、近隣端末が脱退した旨を他の端末に知らせるという作用をもたらす。

【0016】

また、本発明の請求項10記載の端末は、ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルと、上記ネットワークを脱退した端末の

端末識別子を知らせる端末脱退メッセージを受信した場合その脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手段とを具備する。これにより、脱退した端末に関する情報を鍵管理リストテーブルから削除して、未認証状態にするという作用をもたらす。

【0017】

また、本発明の請求項11記載の認証方法は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手順とを具備する。これにより、受信したフレームに付された認証ヘッダが正当な送信端末により生成されたものであることを受信端末に確認させるという作用をもたらす。

【0018】

また、本発明の請求項12記載の認証方法は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵を上記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成する手順と、上記鍵付ハッシュ値と上記フレームの認証ヘッダとを比較することにより上記認証ヘッダが正当であるか否かを確認する手順とを具備する。これにより、強度の保証された鍵付ハッシュ関数に基づいて、受信したフレームに付された認証ヘッダの正当性を受信端末に確認させるという作用をもたらす。

【0019】

また、本発明の請求項13記載の暗号化方法は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リス

トテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手順と、上記認証ヘッダが正当であり且つ上記フレームの終点端末識別子が当該端末の端末識別子である場合上記フレームの始点端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を抽出する手順と、上記抽出されたユニキャスト暗号鍵により上記フレームのペイロードを復号する手順とを具備する。これにより、始点端末と終点端末との間で定められたユニキャスト暗号鍵によりペイロードを暗号化して、中間の端末に対してペイロードの秘匿性を担保するという作用をもたらす。

【0020】

また、本発明の請求項14記載の暗号化方法は、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、送信しようとするフレームの受信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵を上記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成して認証ヘッダとして上記フレームに付する手順と、上記フレームを送信する手順とを具備する。これにより、強度の保証された鍵付ハッシュ関数に基づいて、正当な認証ヘッダが付されていることをフレーム受信端末において確認させるという作用をもたらす。

【0021】

また、本発明の請求項15記載の端末管理方法は、ネットワークを形成する端末のうち直接通信可能な端末の端末識別子を保持する近隣端末リストテーブルと、上記ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルとを備える端末において、上記近隣端末リストテーブルに端末識別子が保持される端末における上記ネットワークからの脱退を検出する手順と、その脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手順と、上記ネットワークを形成する他の端末に対して上記脱退した端末の

端末識別子を知らせる端末脱退メッセージを送信する手順とを具備する。これにより、脱退した近隣端末に関する情報を鍵管理リストテーブルから削除して未認証状態にするとともに、近隣端末が脱退した旨を他の端末に知らせるという作用をもたらす。

【0022】

また、本発明の請求項16記載の端末管理方法は、ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末において、上記ネットワークを脱退した端末の端末識別子を知らせる端末脱退メッセージを受信する手順と、上記脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手順とを具備する。これにより、脱退した端末に関する情報を鍵管理リストテーブルから削除して、未認証状態にするという作用をもたらす。

【0023】

また、本発明の請求項17記載のプログラムは、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手順とを実行させる。これにより、受信したフレームに付された認証ヘッダが正当な送信端末により生成されたものであることを受信端末に確認させるという作用をもたらす。

【0024】

また、本発明の請求項18記載のプログラムは、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵を上記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成する手順と、上記鍵付ハ

ハッシュ値と上記フレームの認証ヘッダとを比較することにより上記認証ヘッダが正当であるか否かを確認する手順とを実行させる。これにより、強度の保証された鍵付ハッシュ関数に基づいて、受信したフレームに付された認証ヘッダの正当性を受信端末に確認させるという作用をもたらす。

【0025】

また、本発明の請求項19記載のプログラムは、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵およびユニキャスト暗号鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、受信したフレームの送信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵により上記フレームの認証ヘッダが正当であるか否かを確認する手順と、上記認証ヘッダが正当であり且つ上記フレームの終点端末識別子が当該端末の端末識別子である場合上記フレームの始点端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記ユニキャスト暗号鍵を抽出する手順と、上記抽出されたユニキャスト暗号鍵により上記フレームのペイロードを復号する手順とを実行させる。これにより、始点端末と終点端末との間で定められたユニキャスト暗号鍵によりペイロードを暗号化して、中間の端末に対してペイロードの秘匿性を担保するという作用をもたらす。

【0026】

また、本発明の請求項20記載のプログラムは、他の端末の端末識別子に対応して上記他の端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、送信しようとするフレームの受信端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから検索して対応する上記認証ヘッダ鍵を抽出する手順と、抽出された上記認証ヘッダ鍵を上記フレームの所定領域と共にハッシュした鍵付ハッシュ値を生成して認証ヘッダとして上記フレームに付する手順と、上記フレームを送信する手順とを実行させる。これにより、強度の保証された鍵付ハッシュ関数に基づいて、正当な認証ヘッダが付されていることをフレーム受信端末において確認させるという作用をもたらす。

【0027】

また、本発明の請求項21記載のプログラムは、ネットワークを形成する端末のうち直接通信可能な端末の端末識別子を保持する近隣端末リストテーブルと、上記ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルとを備える端末に、上記近隣端末リストテーブルに端末識別子が保持される端末における上記ネットワークからの脱退を検出する手順と、その脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手順と、上記ネットワークを形成する他の端末に対して上記脱退した端末の端末識別子を知らせる端末脱退メッセージを送信する手順とを実行させる。これにより、脱退した近隣端末に関する情報を鍵管理リストテーブルから削除して未認証状態にするとともに、近隣端末が脱退した旨を他の端末に知らせるという作用をもたらす。

【0028】

また、本発明の請求項22記載のプログラムは、ネットワークを形成する端末の端末識別子に対応して当該端末との間の認証ヘッダ鍵を保持する鍵管理リストを少なくとも一つ有する鍵管理リストテーブルを備える端末に、上記ネットワークを脱退した端末の端末識別子を知らせる端末脱退メッセージを受信する手順と、上記脱退した端末の端末識別子を含む上記鍵管理リストを上記鍵管理リストテーブルから削除する手順とを実行させる。これにより、脱退した端末に関する情報を鍵管理リストテーブルから削除して、未認証状態にするという作用をもたらす。

【0029】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0030】

図1は、本発明の実施の形態における無線アドホック通信システムのネットワーク構成例である。この例では、端末A、端末B、端末Cおよび端末Dの4つの端末が無線アドホック通信システムのネットワークを構成している。端末A（3

00)からの電波が到達する通信範囲301は、端末Aを中心とする点線により表される。他の端末の通信範囲も同様に表される。この図1の例では、端末Aは端末Bと通信可能であり、端末Bは端末Aおよび端末Cと通信可能であり、端末Cは端末Bおよび端末Dと通信可能であり、端末Dは端末Cと通信可能であることが示されている。従って、例えば端末Aは端末Cや端末Dと直接通信を行うことができず、これら端末CおよびDと通信を行うためには、まず端末Bを介してマルチホップによるフレーム配送を行う必要がある。

【0031】

このような端末を介したフレーム配送を行うためには、認証された正当な端末からフレームを受信したことを確認する必要がある。この処理をフレーム送信元認証という。また、フレームが端末間で配送されると、その経路上でフレームの内容が第三者に傍受されるおそれが生じる。従って、重要な情報の送受やプライベートなやりとりが第三者に傍受されないよう秘匿性を保つ必要が生じる。そこで、本発明の実施の形態では、以下に説明するように、認証ヘッダ鍵を用いたフレーム送信元認証を行うとともに、ユニキャスト暗号鍵を用いた暗号化処理を行う。

【0032】

図2は、本発明の実施の形態におけるフレーム送信元認証および暗号化処理の概要を説明するための図である。フレーム送信の始点である端末Aは、端末Dを終点とするフレームを送信する際、フレーム800のペイロード部802を端末Dとの間のユニキャスト暗号鍵(UK_A_D)により暗号化する。また、端末Aは、次の送信先である端末Bとの間の認証ヘッダ鍵(AHK_A_B)により認証ヘッダ809を生成してフレーム800に付する。

【0033】

フレームを受信した端末Bは、認証ヘッダ809が正当であるか否かを端末Aとの間の認証ヘッダ鍵(AHK_A_B)を用いて確認する。認証ヘッダ809が正当であることが確認されると、端末Bは次の送信先である端末Cとの間の認証ヘッダ鍵(AHK_B_C)により認証ヘッダ809を生成してフレームに付する。その際、暗号化されたペイロード部802はそのまま送信される。一方、認証

ヘッダ 809 が正当でない場合には、そのフレームは次の送信先に配送されることなく破棄される。

【0034】

同様に、フレームを受信した端末 C は、認証ヘッダ 809 が正当であるか否かを端末 B との間の認証ヘッダ鍵 (AHK_B_C) を用いて確認する。認証ヘッダ 809 が正当であることが確認されると、端末 C は次の送信先である端末 D との間の認証ヘッダ鍵 (AHK_CD) により認証ヘッダ 809 を生成してフレームに付する。その際、暗号化されたペイロード部 802 はそのまま送信される。一方、認証ヘッダ 809 が正当でない場合には、そのフレームは次の送信先に配送されることなく破棄される。

【0035】

フレームを受信した端末 D は、認証ヘッダ 809 が正当であるか否かを端末 C との間の認証ヘッダ鍵 (AHK_CD) を用いて確認する。認証ヘッダ 809 が正当であることが確認されると、端末 D はペイロード部 802 を端末 A との間のユニキャスト暗号鍵 (UK_A_D) により復号してその内容を読み出す。一方、認証ヘッダ 809 が正当でない場合には、そのフレームは復号されることなく破棄される。

【0036】

図 3 は、本発明の実施の形態における認証ヘッダ付フレーム 800 の構成を示す図である。フレーム 800 は、ヘッダ部 801 と、ペイロード部 802 とから構成される。ペイロード部 802 には通信の内容であるデータが格納される。このペイロード部 802 が、ユニキャスト暗号鍵による暗号化および復号化の対象となる。

【0037】

ヘッダ部 801 は、始点端末識別子 803 と、終点端末識別子 804 と、送信端末識別子 805 と、受信端末識別子 806 と、フレーム種別 807 と、シーケンス番号 808 と、認証ヘッダ 809 とを含む。始点端末識別子 803 は、このフレームを最初に発信した端末の端末識別子である。なお、端末識別子は、ネットワーク内において端末を一意に識別するものであればよく、例えば、イーサネ

ット（登録商標）におけるMACアドレス等を用いることができる。終点端末識別子804は、このフレームの最終宛先の端末の端末識別子である。

【0038】

送信端末識別子805および受信端末識別子806は、フレームを中継する際に用いられる。無線アドホック通信システムにおいては、ネットワーク内の全ての端末が直接通信できるとは限らず、電波の届かない端末へフレームを送信したい場合には他の端末を介してマルチホップにより通信経路を確立しなければならない。この場合にフレームの送受信を行う端末間で使用されるのが送信端末識別子805および受信端末識別子806である。フレーム種別807は、フレームの種別を示すものである。シーケンス番号808は、フレーム毎に付される一連の順序を表す番号である。

【0039】

認証ヘッダ809は、フレーム送信元認証を行うための認証データである。送信端末と受信端末との間で認証ヘッダ鍵（A H K : A u t h e n t i c a t i o n H e a d e r K e y）を予め定めておき、送信端末において送信フレームの所定領域と認証ヘッダ鍵とを合わせてハッシュした鍵付ハッシュ値を生成して認証ヘッダ809として付する。受信端末では、受信フレームの所定領域と認証ヘッダ鍵とを合わせてハッシュした鍵付ハッシュ値を生成して認証ヘッダ809と比較する。この比較の結果、両者が一致すれば、受信フレームは送信端末から送信されたものであることが確認される。

【0040】

ハッシュの対象となるフレームの所定領域としては、ヘッダ部801の一部を使用することが考えられる。例えば、送信端末識別子805およびシーケンス番号808の組合せ等を使用することが考えられる。シーケンス番号808を組み合わせることにより、いわゆるリプレイ攻撃を防止することができる。

【0041】

図4は、本発明の実施の形態における認証ヘッダを生成する処理の一例を示す流れ図である。上述のハッシュの対象となるフレームの所定領域は、ここではT E X Tとして表される。また、認証ヘッダ鍵は、所定のBバイト（例えば、64

バイト) 長になるよう正規化がされた認証ヘッダ鍵ZAHKが使用される。例えば、所定のBバイトよりも長ければハッシュされる必要があり、また、所定のBバイトよりも短ければゼロが追加される必要がある。なお、ここで用いられるハッシュ関数としては、例えば、MD5 (Message Digest #5) が考えられる。このMD5を用いた鍵付ハッシュ関数は、HMAC-MD5 (Hash-based Message Authentication Code: Keyed MD5) とよばれる。

【0042】

まず、認証ヘッダ鍵ZAHKと固定文字列ipadとの間で排他的論理和が生成される（ステップS992）。この生成された値をIとする。ここで、固定文字列ipadは、例えば、バイト値0x36（ビット列'00110110'）をBバイト分繰り返したものである。そして、この生成された値Iにフレームの所定領域TEXTが追加されて値ITとなる（ステップS993）。この値ITHにハッシュ関数が適用されて第1のハッシュ値ITHが生成される（ステップS994）。

【0043】

また、認証ヘッダ鍵ZAHKと固定文字列opadとの間で排他的論理和が生成される（ステップS995）。この生成された値をOとする。ここで、固定文字列opadは、例えば、バイト値0x5c（ビット列'01011100'）をBバイト分繰り返したものである。そして、この生成された値Oに第1のハッシュ値ITHが追加されて値OITHとなる（ステップS996）。この値OITHにハッシュ関数が適用されて第2のハッシュ値として認証ヘッダAHが生成される（ステップS997）。

【0044】

なお、この図4の手順は、フレーム送信端末において認証ヘッダを付する際に使用されるだけでなく、フレームに付された認証ヘッダが正当であるか否かをフレーム受信端末において確認する際にも使用される。すなわち、フレーム受信端末において上述の第2のハッシュ値を生成して、それがフレームに付された認証ヘッダと一致すればその認証ヘッダは正当であることが確認される。

【0045】

図5は、本発明の実施の形態における無線アドホック通信システムにおいて使用される無線端末300の構成例を示す図である。無線端末300は、通信処理部320と、制御部330と、表示部340と、操作部350と、スピーカ360と、マイク370と、メモリ600とを備え、これらの間をバス380が接続する構成となっている。また、通信処理部320にはアンテナ310が接続されている。通信処理部320は、アンテナ310を介して受信した信号からネットワークインターフェース層（データリンク層）のフレームを構成する。また、通信処理部320は、ネットワークインターフェース層のフレームをアンテナ310を介して送信する。

【0046】

制御部330は、無線端末300全体を制御する。例えば、通信処理部320により構成されたフレームを参照して所定の処理を行う。また、制御部330は、タイマ335を有し、所定のイベントからの経過時間を計時する。表示部340は、所定の情報を表示するものであり、例えば、液晶ディスプレイ等が用いられる。操作部350は、無線端末300に対して外部から操作指示を行うためのものであり、例えば、キーボードやボタンスイッチ等が用いられる。スピーカ360は、音声を出力するものであり、無線端末300の利用者に対して注意を喚起したり他の端末と音声情報のやりとりを行うために用いられる。マイク370は、無線端末300に対して外部から音声入力を行うものであり、他の端末と音声情報のやりとりを行ったり操作指示を行うために用いられる。

【0047】

メモリ600は、無線端末300自身の生成鍵に関する情報として自端末の公開鍵および秘密鍵や公開鍵証明書等を保持する生成鍵テーブル650と、他の端末との間のユニキャスト暗号鍵および認証ヘッダ鍵を保持する鍵管理リストテーブル670と、終点端末にフレームを到達させるための転送先端末に関する情報を保持する経路テーブル680と、ネットワークを形成する端末のうち直接通信可能な端末に関する情報を保持する近隣端末リストテーブル690とを格納する。

【0048】

図6は、本発明の実施の形態における鍵管理リストテーブル670の構成例である。この鍵管理リストテーブル670は、暗号化ならびに復号化に用いられるユニキャスト鍵および認証ヘッダ生成に用いられる認証ヘッダ鍵を保持するものであり、他の端末の端末識別子671に対応して当該他の端末との間のユニキャスト暗号鍵672および認証ヘッダ鍵673を保持する鍵管理リストを少なくとも一つ有する。

【0049】

端末識別子671は、上述の通り他の端末を一意に識別するものであり、一例としてMACアドレス等を用いることができる。ユニキャスト暗号鍵672は、対応する端末識別子671を有する端末との間のユニキャスト通信のために定められた共通鍵である。このユニキャスト暗号鍵672を表すために、例えば、端末Aと端末Bとの間で使用されるユニキャスト暗号鍵を「UK_AB」等と表記する。

【0050】

なお、このユニキャスト暗号鍵に用いられる共通鍵アルゴリズムとしては、56ビットの鍵の長さを有するDES(Data Encryption Standard)、128ビット、192ビットおよび256ビットの3通りの鍵の長さを有するAES(Advanced Encryption Standard)等が知られている。

【0051】

認証ヘッダ鍵673は、認証ヘッダを生成するために使用される共有秘密鍵である。認証ヘッダ鍵673は、フレームの所定領域と共にハッシュされ、間に割り込もうとする組織が認証ヘッダを複製することを不可能にする。この認証ヘッダ鍵673は、できるだけ頻繁に変更されるべきである。この認証ヘッダ鍵673は、無作為に選ばれるか、ランダムな種を与えた暗号的に強い擬似乱数発生器を使用して生成される。

【0052】

図7は、本発明の実施の形態における経路テーブル680の構成例である。こ

の経路テーブル680は、終点端末にフレームを到達させるための転送先端末に関する情報を保持するものであり、終点端末の端末識別子681に対応してフレームの転送先端末の端末識別子682および有効時間683を保持する経路リストを少なくとも一つ有する。

【0053】

終点端末識別子681および転送先端末識別子682における端末識別子は、上述の通り他の端末を一意に識別するものである。ある端末に最終的にフレームを配送するために、次にどの端末にフレームを転送すべきであるかを示している。図7の例は図1のネットワーク構成例を想定したものであり、端末Aから何れの端末にフレームを配送する場合であっても、まずは端末Bにフレームを転送することになる。

【0054】

無線アドホック通信システムにおいては、ネットワーク構成が時々刻々と変化する可能性がある。従って、経路テーブル680に保持される情報も古くなる可能性がある。そこで、有効時間683によって、対応する情報の鮮度を管理する。例えば、情報更新時もしくは情報更新からの経過時間を有効時間683に記録していくことにより、所定時間以上経過した情報を削除もしくは更新することが考えられる。これらの時間を計時するために制御部330のタイマ335が使用される。

【0055】

図8は、本発明の実施の形態における近隣端末リストテーブル690の構成例である。この近隣端末リストテーブル690は、無線アドホック通信システムにおいてネットワークを形成する端末のうち直接通信可能な近隣端末に関する情報を保持するものであり、近隣端末の端末識別子691に対応して有効時間692を保持する近隣端末リストを少なくとも一つ有する。

【0056】

近隣端末識別子691は、近隣端末を一意に識別するものである。例えば、各端末が自己の存在を示すビーコンを定期的に発生するものとして、ビーコンを受信した端末は、そのビーコンに含まれる送信端末識別子805（図3）によって

ビーコン送信端末の端末識別子を知ることができる。そこで、ビーコン受信端末は、このようにして取得したビーコン送信端末の端末識別子を近隣端末リストテーブル 690 の近隣端末識別子 691 に保持する。なお、本発明の実施の形態において、ビーコンは、標識信号としてのビーコン情報のみを含む信号だけではなく、ビーコン情報に何らかのデータ情報が付加された信号をも含む。

【0057】

無線アドホック通信システムにおいては、ネットワーク構成が時々刻々と変化する可能性がある。それまで存在していた近隣端末が通信範囲外へ移動する場合やネットワークから離脱する場合もある。そこで、有効時間 692 によって、対応する近隣端末の認証状態を管理する。例えば、ビーコン受信時もしくはビーコン受信からの経過時間を有効時間 692 に記録していくことにより、所定時間以上経過した近隣端末はネットワークから離脱したものと判断することが考えられる。このビーコン受信からの経過時間を計時するために制御部 330 のタイマ 335 が使用される。

【0058】

次に本発明の実施の形態における無線アドホック通信システムの動作について図面を参照して説明する。本発明の実施の形態では、端末がネットワーク資源に接続する際に端末間で相互認証を行っていることを想定する。そして、相互認証に続く以下の鍵配布シーケンスにより認証ヘッダ鍵（図 9）やユニキャスト暗号鍵（図 10）を共有する。これら図 9 および図 10 における各処理は、無線端末 300 における制御部 330 により実現される。

【0059】

図 9 は、本発明の実施の形態における認証ヘッダ鍵配布の手順を示す図である。この図 9 の例では端末 A（100）および端末 B（200）のうち、端末 A が認証ヘッダ鍵を生成しているが、これは何れの端末が生成しても構わない。例えば、端末識別子の大小により決定するようにしてもよい。

【0060】

まず、端末 A は、認証ヘッダ鍵を配布するために必要な公開鍵を保持しているか否かを判断する。もし、端末 B の公開鍵を有していない場合には、端末 B に対

して公開鍵を要求する公開鍵要求メッセージ1312を送信する（131）。この公開鍵要求メッセージ1312は、図3で説明した構成のフレームを用いることができるが、この時点ではまだ認証ヘッダを付することはできない。

【0061】

公開鍵要求メッセージ1312を受信した端末Bは、生成鍵テーブル650（図5）に保持された端末Bの公開鍵（PK_B）を公開鍵配布メッセージ2321により端末Aに送信する（232）。この公開鍵要求メッセージ2321も、図3で説明したフレーム構成を用いることができる。公開鍵配布メッセージ2321を受信した端末Aは、端末Bの公開鍵（PK_B）を取り出す。

【0062】

また、端末Aは、認証ヘッダ鍵（AHK_AB）を生成する（133）。認証ヘッダ鍵は、上述のように、無作為もしくは乱数により生成される。また、この認証ヘッダ鍵は、適宜変更されるべきものである。端末Aは、生成した認証ヘッダ鍵（AHK_AB）を端末Bの公開鍵（PK_B）により暗号化して認証ヘッダ鍵配布メッセージ1342として端末Bに送信する（134）。認証ヘッダ鍵配布メッセージ1342を受信した端末Bは、端末B自身の秘密鍵により認証ヘッダ鍵を復号する（234）。

【0063】

端末Aおよび端末Bは、このようにして取得した認証ヘッダ鍵（AHK_AB）を、自端末の鍵管理リストテーブル670（図6）に設定する（135、235）。すなわち、端末Aは端末識別子671として端末Bを有する鍵管理リストの認証ヘッダ鍵673欄に認証ヘッダ鍵（AHK_AB）を設定し、端末Bは端末識別子671として端末Aを有する鍵管理リストの認証ヘッダ鍵673欄に認証ヘッダ鍵（AHK_AB）を設定する。このようにして、無線アドホック通信システムのネットワークを構成する各端末は、隣接端末との間で認証ヘッダ鍵を共有する。

【0064】

図10は、本発明の実施の形態におけるユニキャスト暗号鍵配布の手順を示す図である。このユニキャスト暗号鍵は予め配布しておいてもよいが、実際に通信

を行う際に配布するようにしてもよい。この図10の例では端末A（100）および端末D（400）のうち、端末Aがユニキャスト暗号鍵を生成しているが、これは何れの端末が生成しても構わない。例えば、端末識別子の大小により決定するようにしてもよい。

【0065】

まず、端末Aは、ユニキャスト暗号鍵を配布するために必要な公開鍵を保持しているか否かを判断する。もし、端末Dの公開鍵を有していない場合には、端末Dに対して公開鍵を要求する公開鍵要求メッセージ1414を送信する（141）。この公開鍵要求メッセージ1414は、図3で説明した構成のフレームを用いることができる。

【0066】

公開鍵要求メッセージ1414を受信した端末Dは、生成鍵テーブル650（図5）に保持された端末Dの公開鍵（PK_D）を公開鍵配布メッセージ4421により端末Aに送信する（442）。この公開鍵要求メッセージ4421も、図3で説明したフレーム構成を用いることができる。公開鍵配布メッセージ4421を受信した端末Aは、端末Dの公開鍵（PK_D）を取り出す。

【0067】

また、端末Aは、ユニキャスト暗号鍵（UK_A D）を生成する（143）。ユニキャスト暗号鍵は、無作為もしくは乱数により生成される。端末Aは、生成したユニキャスト暗号鍵（UK_A D）を端末Dの公開鍵（PK_D）により暗号化してユニキャスト暗号鍵配布メッセージ1444として端末Dに送信する（144）。ユニキャスト暗号鍵配布メッセージ1444を受信した端末Dは、端末D自身の秘密鍵によりユニキャスト暗号鍵を復号する（444）。

【0068】

端末Aおよび端末Dは、このようにして取得したユニキャスト暗号鍵（UK_A D）を、自端末の鍵管理リストテーブル670（図6）に設定する（145、245）。すなわち、端末Aは端末識別子671として端末Dを有する鍵管理リストのユニキャスト暗号鍵672欄にユニキャスト暗号鍵（UK_A D）を設定し、端末Dは端末識別子671として端末Aを有する鍵管理リストのユニキャス

ト暗号鍵672欄にユニキャスト暗号鍵（UK_A_D）を設定する。

【0069】

次に本発明の実施の形態における無線アドホック通信システムの各端末におけるフレーム送受信処理について図面を参照して説明する。

【0070】

図11は、本発明の実施の形態におけるフレーム送信の際の処理を示す図である。自端末を始点とするフレームを送信する場合には、始点端末識別子803が自端末の端末識別子となるので（ステップS951）、終点端末との間で定められたユニキャスト暗号鍵によりペイロード部802を暗号化する（ステップS952）。このユニキャスト暗号鍵は、終点端末識別子804と一致する端末識別子671に対応するユニキャスト暗号鍵672を図6の鍵管理リストテーブル670から抽出することにより得られる。他の端末からのフレームを中継する場合には、始点端末識別子803は自端末の端末識別子と異なるので、ペイロード部802には何も加工を施さない（ステップS951）。

【0071】

そして、受信端末との間の認証ヘッダ鍵により認証ヘッダが生成され、フレーム800の認証ヘッダ809（図3）に付される（ステップS953）。この認証ヘッダ鍵は、受信端末識別子806（図3）と一致する端末識別子671に対応する認証ヘッダ鍵673を図6の鍵管理リストテーブル670から抽出することにより得られる。その後、認証ヘッダが付されたフレームは下位層に送出される（ステップS954）。

【0072】

図12は、本発明の実施の形態におけるフレーム受信の際の処理を示す図である。認証ヘッダ付フレームを受信した端末は、送信端末との間の認証ヘッダ鍵を抽出して（ステップS961）、この認証ヘッダ鍵を用いてフレームに付された認証ヘッダ809が正当であるか否かを確認する（ステップS962）。この認証ヘッダ鍵は、送信端末識別子805（図3）と一致する端末識別子671に対応する認証ヘッダ鍵673を図6の鍵管理リストテーブル670から抽出することにより得られる。認証ヘッダが正当でなければ（ステップS962）、当該フ

レームは破棄される（ステップS963）。

【0073】

認証ヘッダが正当であり（ステップS962）、終点端末識別子が自端末の端末識別子であれば（ステップS964）、始点端末識別子803（図3）と一致する端末識別子671に対応するユニキャスト暗号鍵672を図6の鍵管理リストテーブル670から抽出して、そのユニキャスト暗号鍵によりペイロード部802を復号する（ステップS965）。復号されたフレームは上位層において処理される（ステップS966）。

【0074】

一方、認証ヘッダが正当であり（ステップS962）、終点端末識別子が自端末の端末識別子でなければ（ステップS964）、そのフレームは次点の端末へ転送される（ステップS967）。次点の端末は、フレーム800の終点端末識別子804（図3）と一致する終点端末識別子681を経路テーブル680（図7）から抽出して、対応する転送先端末識別子682を参照することにより知ることができる。

【0075】

次に本発明の実施の形態における無線アドホック通信システムのネットワークから端末が離脱する際の処理について説明する。

【0076】

各端末は、近隣端末リストテーブル690に保持された端末識別子を有する端末との間で通信を行うことにより、無線アドホック通信システムのネットワークを構成する。ある端末がネットワークから離脱する場合としては、その端末が明示的に離脱を宣言することにより脱退する場合や、端末の物理的位置が変動したり電源が切断したことによる通信のタイムアウト等により非明示的に脱退する場合が考えられる。

【0077】

端末が明示的に離脱する場合は、例えば、離脱しようとする端末が離脱要求メッセージを近隣端末に送信することにより離脱を宣言することにより生じ得る。この離脱要求メッセージのフレーム構成は、図3と同様であり、適切な認証ヘッ

ダおよび暗号化処理がなされる。従って、悪意のある端末がなりすまして離脱要求メッセージを送信することはできない。離脱要求メッセージを受信した端末は、その送信元端末に対して離脱応答メッセージを返信する。これにより、端末が明示的に離脱される。

【0078】

端末が非明示的に離脱する場合は、例えば、ある端末の存在を近隣端末が確認できなくなったことにより生じ得る。各端末は、定期的にビーコンを送信しており、近隣端末からのビーコンを受信すると近隣端末リストテーブル 690 を更新する。例えば、端末の移動等により近隣端末との物理的な距離が広がって電波到達範囲（通信範囲）より外に出てしまった場合や、バッテリー切れ等の突発的な電源切断等により相手端末との通信を行うことができなくった場合には、ビーコンを受信することができなくなり、近隣端末リストテーブル 690 の更新が行われなくなる。近隣端末リストテーブル 690 の更新が所定時間以上行われなくなった近隣端末については認証関係をリセットし、未認証状態にする。これにより、端末が非明示的に離脱される。

【0079】

図 13 は、端末が明示的に離脱する際の手順を示す図である。端末 A は、ネットワークから離脱する場合には、離脱要求メッセージ 1512 を送信する（151）。この離脱要求メッセージ 1512 のフレーム構成は図 3 の通りであり、近隣端末である端末 B を受信端末識別子 806 および終点端末識別子 804 とする。端末 B は、この離脱要求メッセージ 1512 を受信すると（251）、端末 A に対して離脱応答メッセージ 2521 を送信する（252）。この離脱応答メッセージ 2521 も図 3 の通りであり、端末 A を受信端末識別子 806 および終点端末識別子 804 とする。端末 A は、この離脱応答メッセージ 2521 を受信（152）することにより、離脱要求が受領されたことを確認する。

【0080】

図 14 は、離脱要求メッセージを受信した端末、もしくは、非明示的な離脱を検出した端末が行う動作を示す図である。離脱要求メッセージを受信し、もしくは、非明示的な離脱を検出すると、近隣端末リストテーブル 690 を参照して、

離脱端末以外に端末が存在すれば（ステップS971）、端末脱退メッセージをブロードキャストする（ステップS972）。この端末脱退メッセージのフレーム構成は図3の通りであり、受信端末識別子806に近隣端末の端末識別子が設定され、終点端末識別子804にはブロードキャストアドレスが設定される。また、ペイロード部802には脱退する端末の端末識別子が含まれる。

【0081】

そして、鍵管理リストテーブル670の端末識別子671において離脱端末の端末識別子を有する鍵管理リストを抽出し、該当する鍵管理リストを削除する（ステップS973）。これにより、当該端末との間で認証ヘッダを交換することができなくなり、また、暗号化されたフレームを交換することもできなくなる。従って、一旦離脱した端末が再度接続しようとしてもそのままの状態では接続することはできない。

【0082】

図15は、離脱脱退メッセージを受信した端末が行う動作を示す図である。離脱脱退メッセージを受信すると、予め保持していたブロードキャスト暗号鍵によりその離脱脱退メッセージを復号して（ステップS981）、ペイロード部802から脱退する端末の端末識別子を取り出す。そして、鍵管理リストテーブル670の端末識別子671において離脱端末の端末識別子を有する鍵管理リストを抽出し（ステップS982）、該当する鍵管理リストを削除する（ステップS983）。これにより、離脱端末は、ネットワーク上の何れの端末との間でも認証ヘッダを交換することができなくなり、また、暗号化されたフレームを交換することもできなくなる。従って、一旦離脱した端末が再度接続しようとしてもそのままの状態ではその接続を受け付けることはできない。

【0083】

このように、本発明の実施の形態によれば、送信端末においてフレーム800のヘッダ部801に認証ヘッダ鍵を用いて生成した認証ヘッダ809を付しておき、受信端末において認証ヘッダ鍵を用いて認証ヘッダ809の正当性を確認することにより、そのフレーム800が認証された正当な端末から送信されたものであることを確認することができる。また、これにより、不要な通信を回避する

ことができ、無線資源の浪費を未然に防止することができる。

【0084】

なお、ここでは本発明の実施の形態を例示したものであり、本発明はこれに限られず、本発明の要旨を逸脱しない範囲において種々の変形を施すことができる。

【0085】

また、ここで説明した処理手順はこれら一連の手順を有する方法として捉えてもよく、これら一連の手順をコンピュータ（端末）に実行させるためのプログラム乃至そのプログラムを記憶する記録媒体として捉えてもよい。

【0086】

【発明の効果】

以上の説明で明らかなように、本発明によると、無線アドホック通信システムにおいて、配送にかかる端末間でフレーム送信元認証を行うことができるという効果が得られる。

【図面の簡単な説明】

【図1】

本発明の実施の形態における無線アドホック通信システムのネットワーク構成例である。

【図2】

本発明の実施の形態におけるフレーム送信元認証および暗号化処理の概要を説明するための図である。

【図3】

本発明の実施の形態における認証ヘッダ付フレーム800の構成を示す図である。

【図4】

本発明の実施の形態における認証ヘッダを生成する処理の一例を示す流れ図である。

【図5】

本発明の実施の形態における無線アドホック通信システムにおいて使用される

無線端末300の構成例を示す図である。

【図6】

本発明の実施の形態における鍵管理リストテーブル670の構成例を示す図である。

【図7】

本発明の実施の形態における経路テーブル680の構成例を示す図である。

【図8】

本発明の実施の形態における近隣端末リストテーブル690の構成例を示す図である。

【図9】

本発明の実施の形態における認証ヘッダ鍵配布の手順を示す図である。

【図10】

本発明の実施の形態におけるユニキャスト暗号鍵配布の手順を示す図である。

【図11】

本発明の実施の形態におけるフレーム送信の際の処理を示す図である。

【図12】

本発明の実施の形態におけるフレーム受信の際の処理を示す図である。

【図13】

本発明の実施の形態において端末が明示的に離脱する際の手順を示す図である。

。

【図14】

本発明の実施の形態における離脱要求メッセージを受信した端末、もしくは、非明示的な離脱を検出した端末が行う動作を示す図である。

【図15】

本発明の実施の形態における離脱脱落メッセージを受信した端末が行う動作を示す図である。

【符号の説明】

300 無線端末

301 通信範囲

310 アンテナ
320 通信処理部
330 制御部
335 タイマ
340 表示部
350 操作部
360 スピーカ
370 マイク
380 バス
600 メモリ
650 生成鍵テーブル
670 鍵管理リストテーブル
671 端末識別子
672 ユニキャスト暗号鍵
673 認証ヘッダ鍵
680 経路テーブル
681 終点端末識別子
682 転送先端末識別子
683 有効時間
690 近隣端末リストテーブル
691 近隣端末識別子
692 有効時間
800 認証ヘッダ付フレーム
801 ヘッダ部
802 ペイロード部
803 始点端末識別子
804 終点端末識別子
805 送信端末識別子
806 受信端末識別子

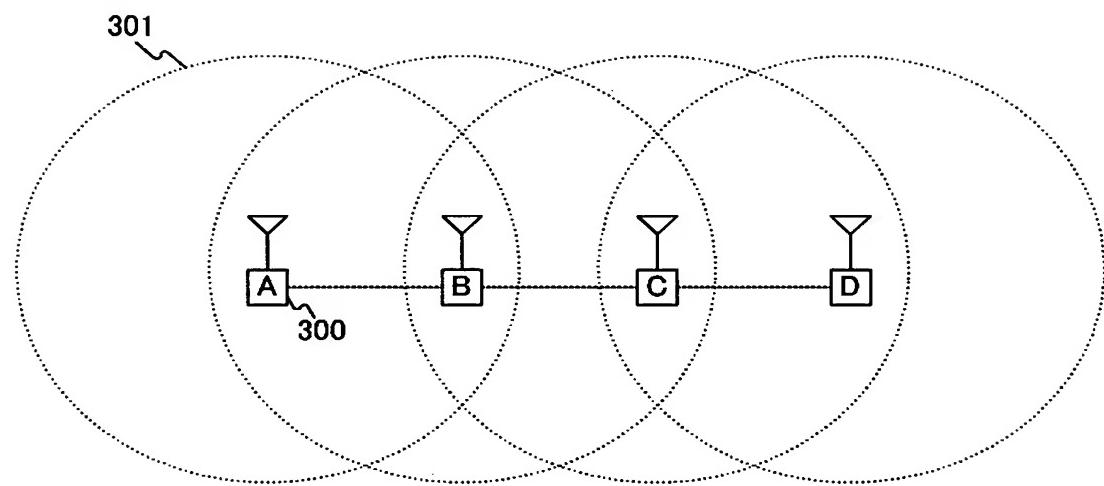
807 フレーム種別

808 シーケンス番号

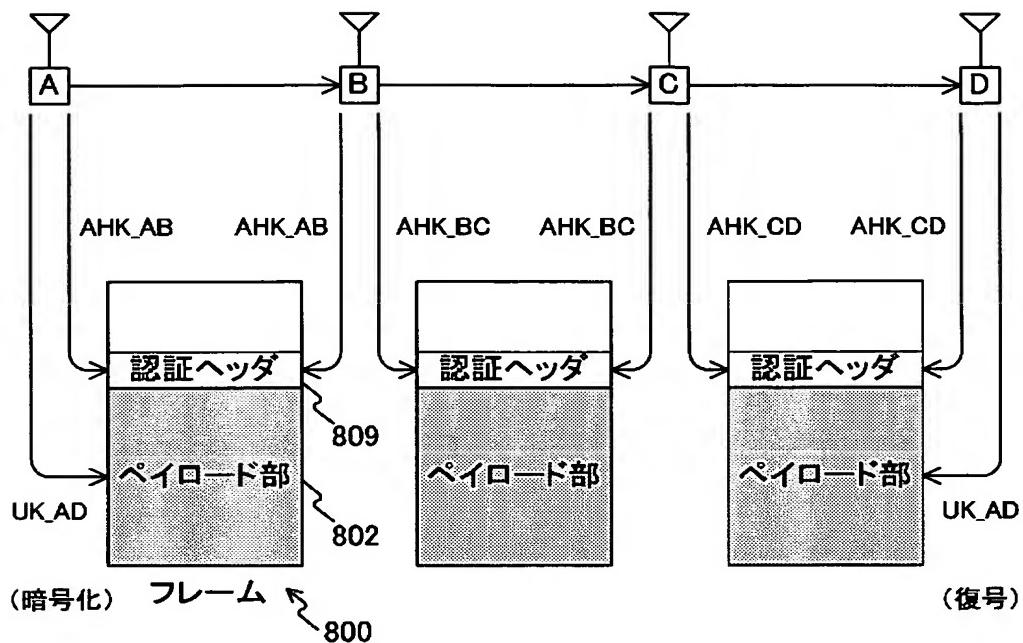
809 認証ヘッダ

【書類名】 図面

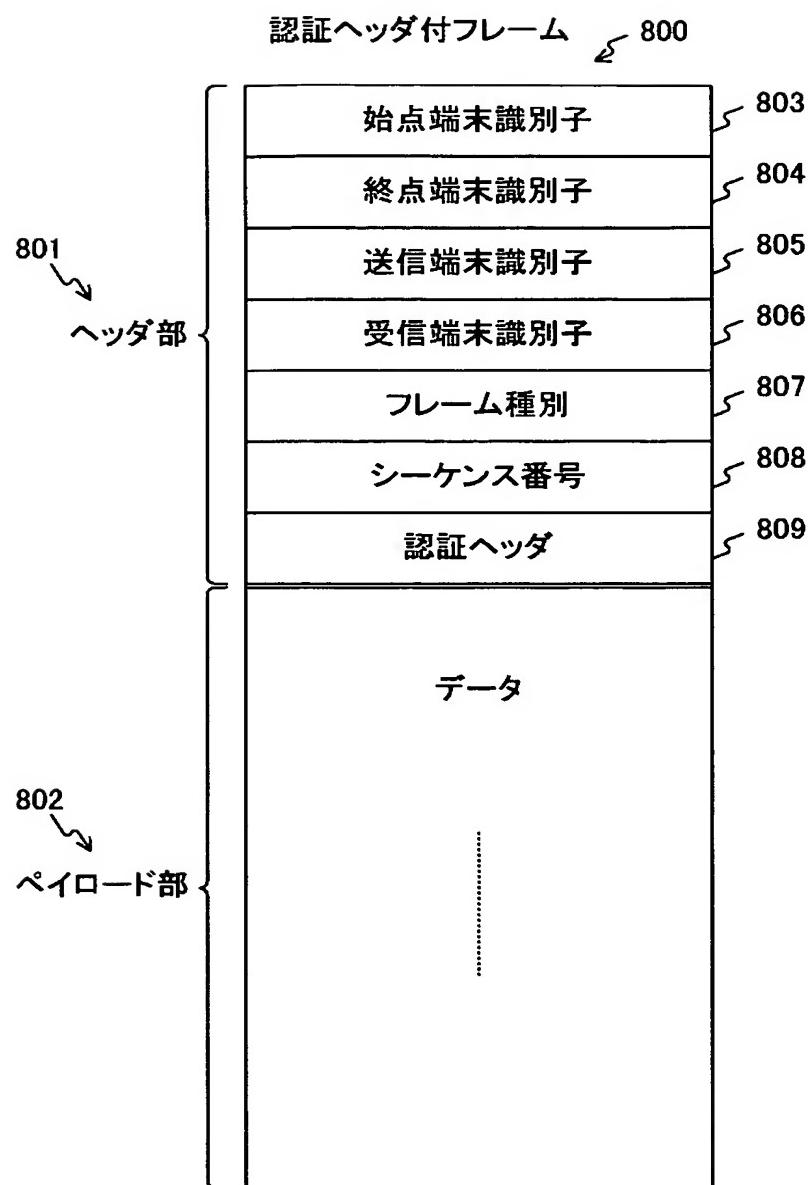
【図 1】



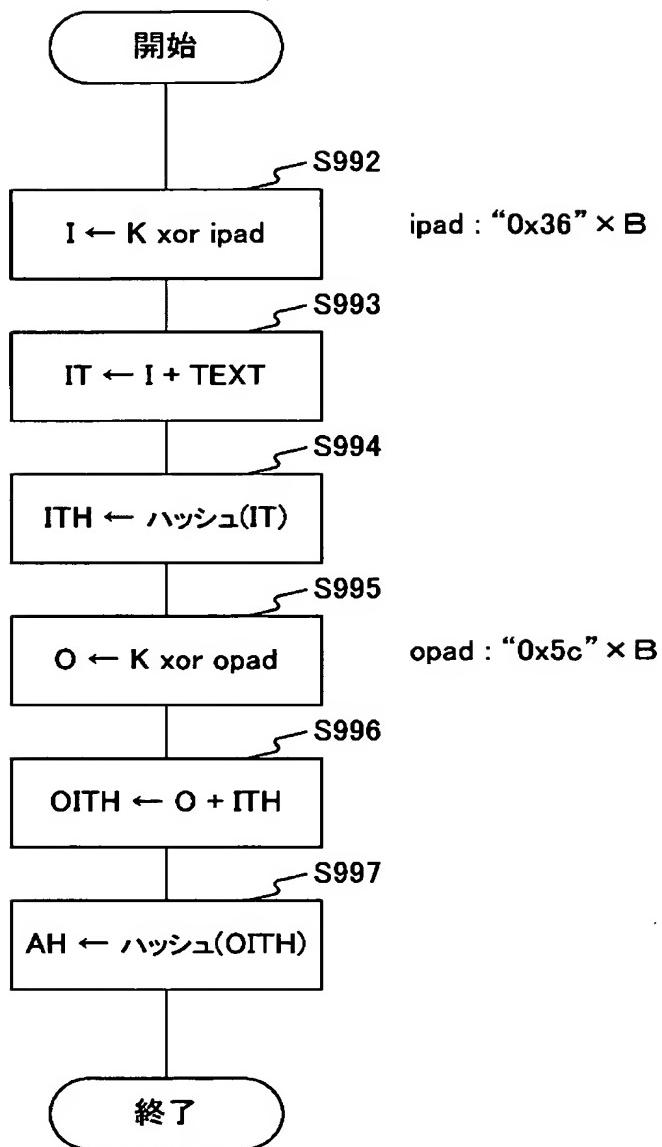
【図 2】



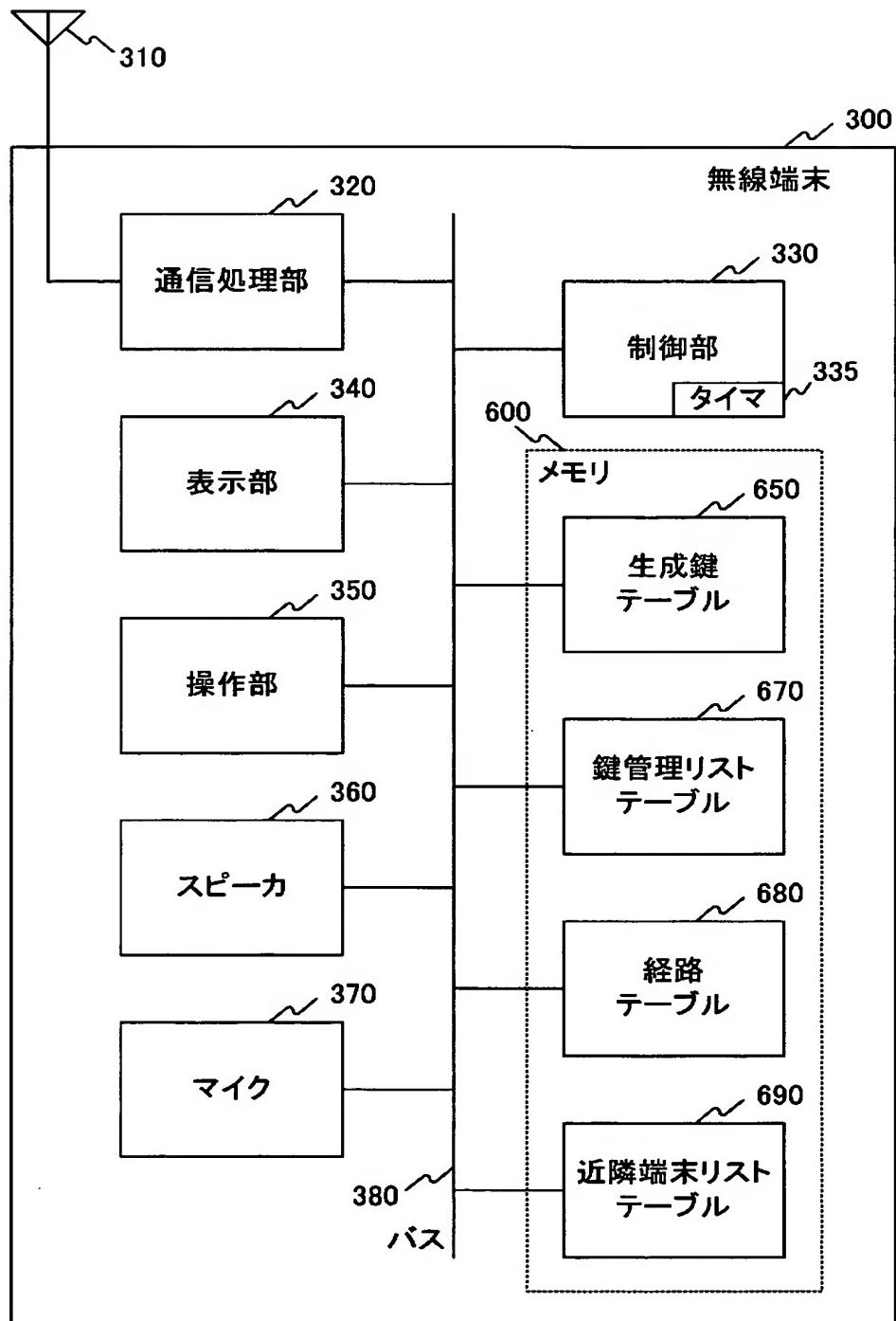
【図3】



【図 4】



【図 5】



【図 6】

鍵管理リストテーブル 670

~ 671 端末識別子 ~ 672 ユニキャスト暗号鍵 ~ 673 認証ヘッダ鍵

端末B	UK_AB	AHK_AB
端末C	UK_AC	AHK_AC
端末D	UK_AD	AHK_AD
⋮	⋮	⋮

【図7】

経路テーブル

680

681 682 683

終点端末識別子	転送先端末識別子	有効時間
端末B	端末B	1:30
端末C	端末B	0:50
端末D	端末B	0:30
⋮	⋮	⋮

【図 8】

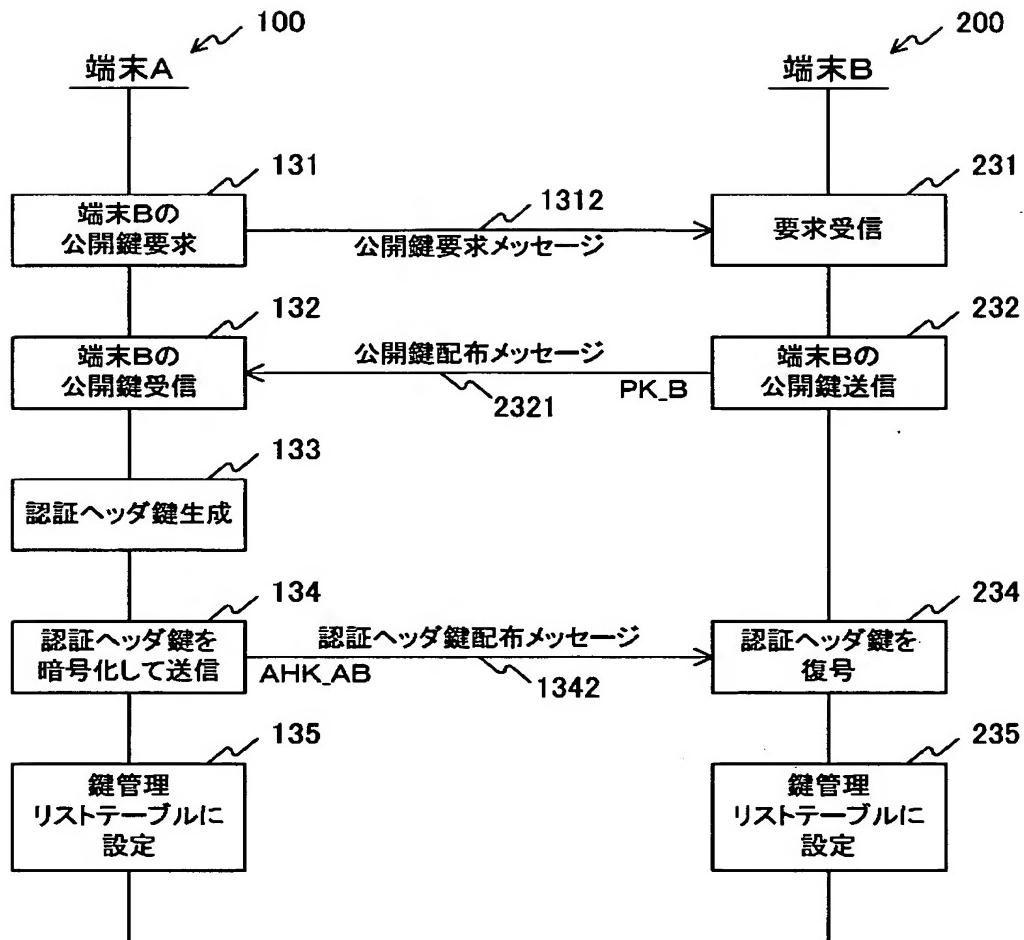
近隣端末リストテーブル 690

~~691 ~~692

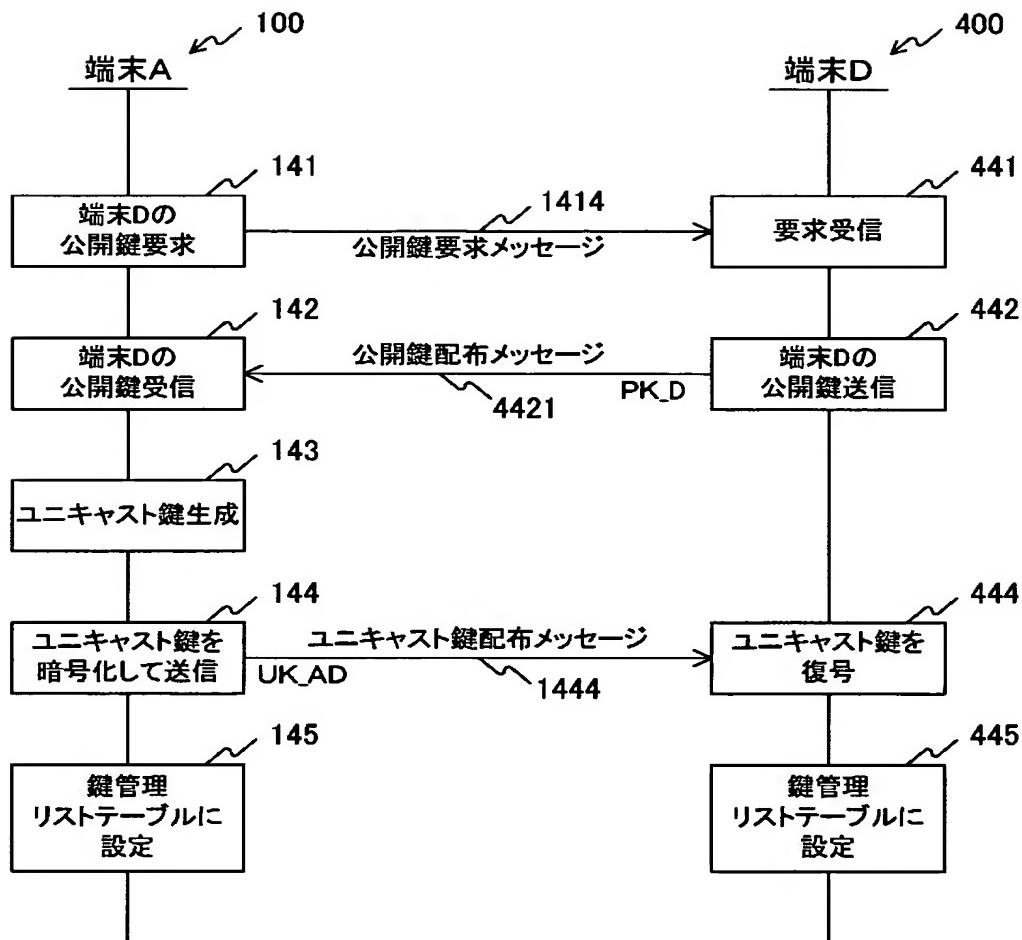
近隣端末識別子 有効時間

端末A	1:30
端末C	0:50

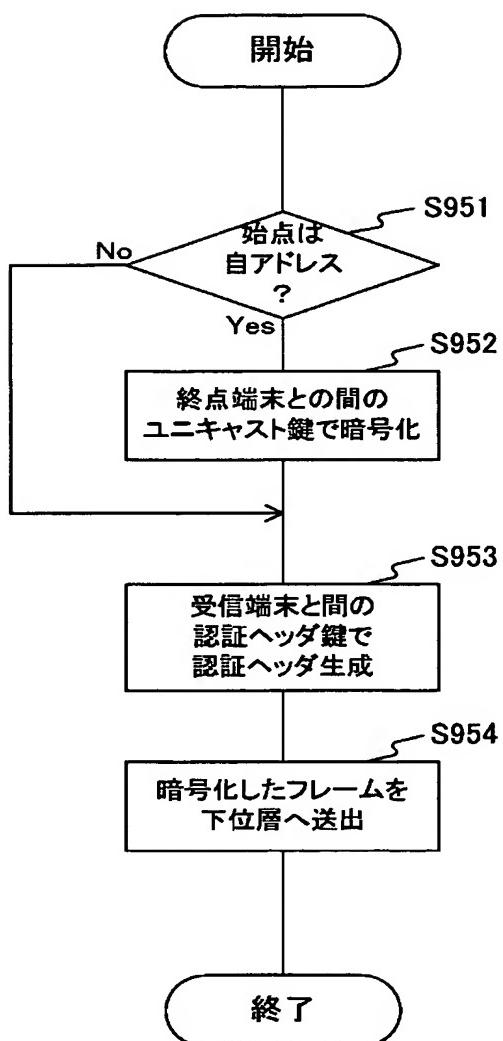
【図 9】



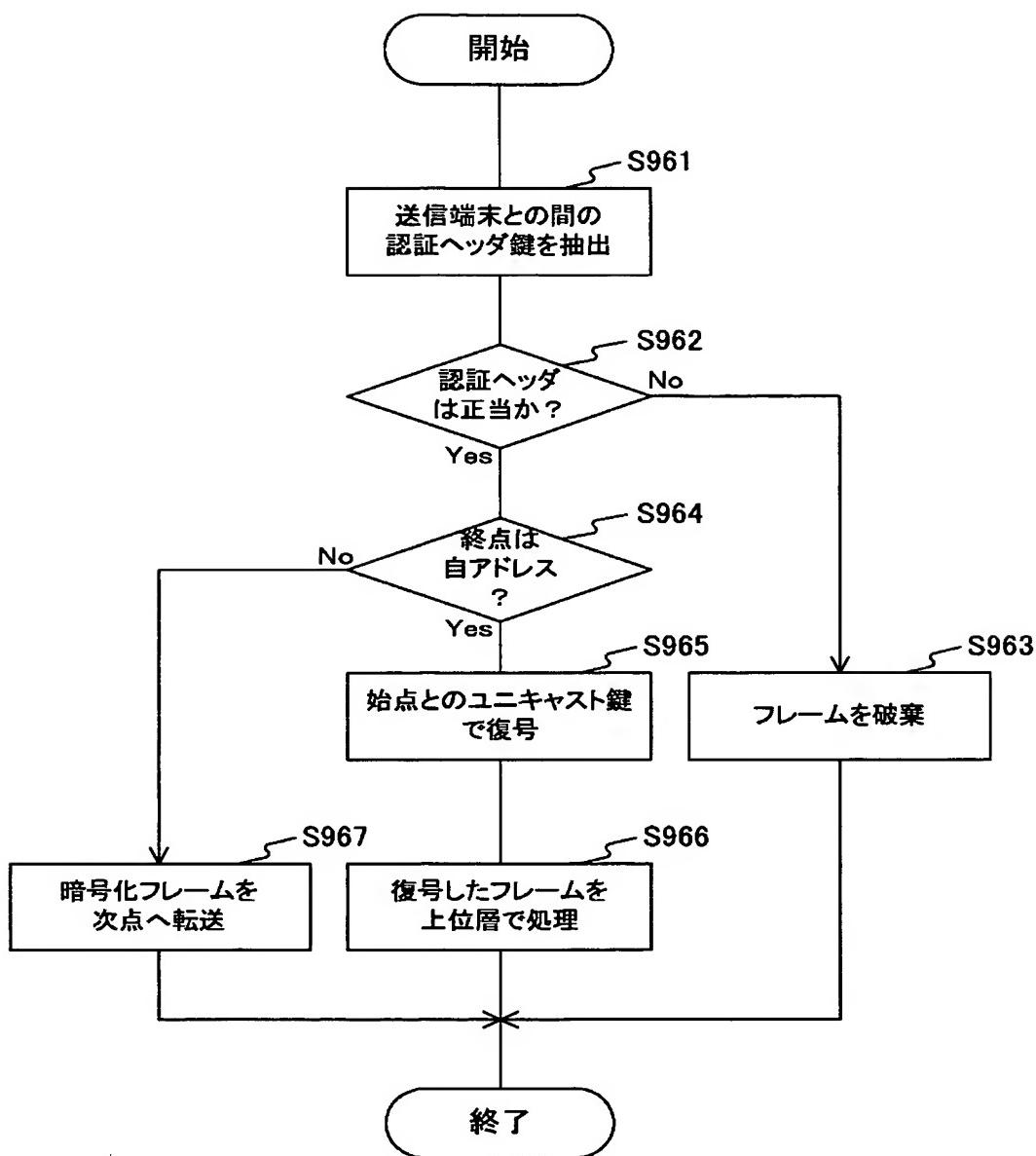
【図 10】



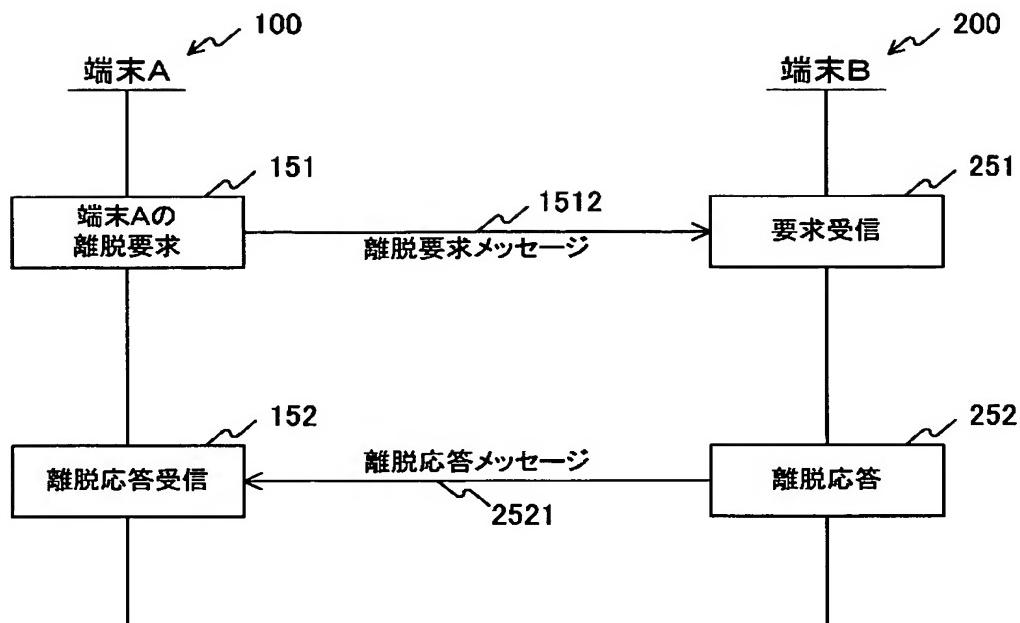
【図 11】



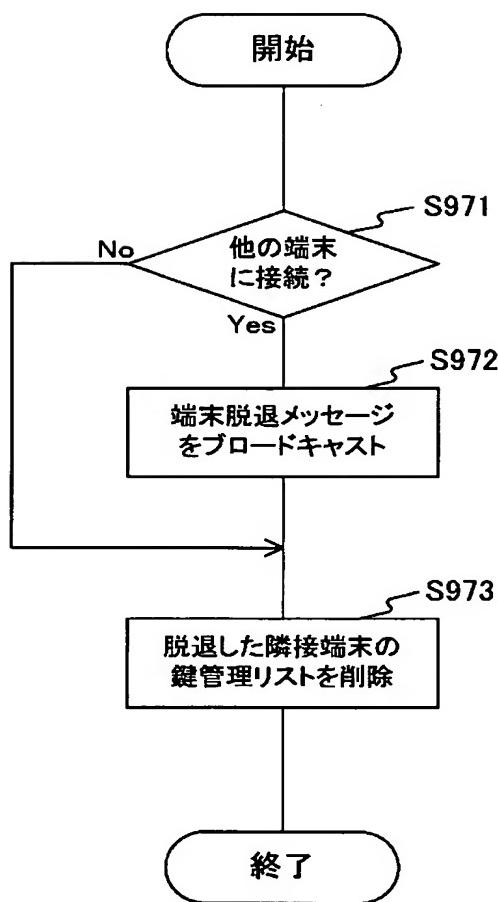
【図12】



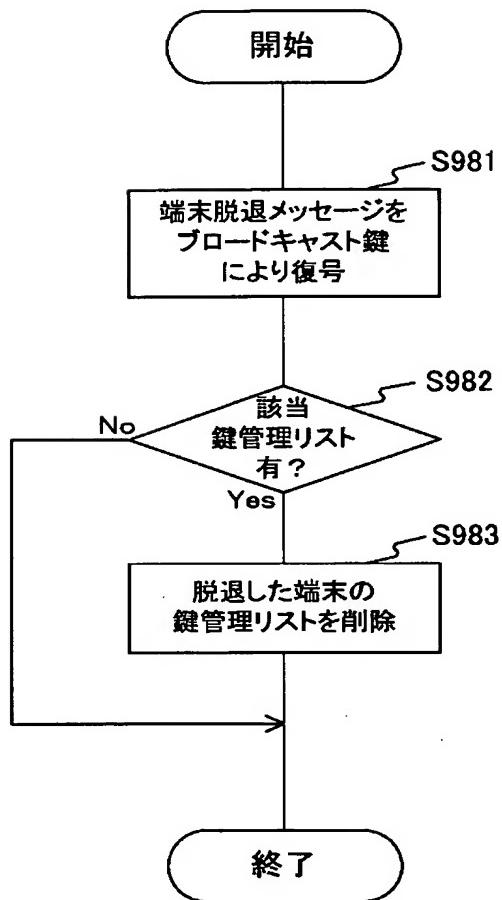
【図13】



【図 14】



【図15】



【書類名】 要約書

【要約】

【課題】 無線アドホック通信システムにおいて、配送にかかる端末間でフレーム送信元認証を行う。

【解決手段】 端末Aは端末Bとの間で定めた認証ヘッダ鍵A H K_A Bを用いて鍵付ハッシュ値を生成して、フレーム800の認証ヘッダ809に付する。端末Bは端末Aとの間で定めた認証ヘッダ鍵A H K_A Bを用いて鍵付ハッシュ値を生成して、フレーム800に付された認証ヘッダ809と比較する。端末Bにおいて生成した鍵付ハッシュ値と認証ヘッダ809とが一致すれば、当該フレーム800は認証された正当な端末Aから送信されたものであることが確認される。また、端末Aは端末Dとの間で定めたユニキャスト暗号鍵U K_A Dを用いてペイロード部802を暗号化する。この暗号化されたペイロード部802は、ユニキャスト暗号鍵U K_A Dを有する端末Dだけが復号できる。

【選択図】 図2

特願 2003-026545

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住所 東京都品川区北品川6丁目7番35号
氏名 ソニー株式会社